Senate Judiciary Committee
Subcommittee on Technology, Terrorism, and Government Information

Senator Jon Kyl, Chair

July 12, 2000

Testimony of

Steven M. Emmert
Director, Government and Industry Affairs
Reed Elsevier Inc. and LEXIS-NEXIS

President, Individual Reference Services Group

Individual Privacy and Industry Self-Regulatory Activities

I. Introduction

I am the Director of Government and Industry Affairs for Reed Elsevier Inc. and LEXIS-NEXIS, a wholly owned division of Reed Elsevier. On behalf of both LEXIS-NEXIS and the Individual Reference Services Group, I very much appreciate the opportunity to testify before your Committee about the information practices of my company, our efforts in the area of acquisition, security, and use of personally identifiable information from non-public sources, and industry's leadership efforts to balance privacy protections with legitimate, socially beneficial information needs.

LEXIS-NEXIS leads the information industry with the largest one-stop, dial-up information service, the LEXIS-NEXIS service for legal, business, and government professionals. The LEXIS-NEXIS service contains more than 2.2 trillion characters and approximately 2.5 billion documents in more than 10,200 databases. It adds 14.7 million documents each week.

Today, two million professionals worldwide–lawyers, accountants, financial analysts, journalists, law enforcement officials, and information specialists–subscribe to the LEXIS-NEXIS services. They perform more than 400,000 searches per day. The combined services contain more than 24,800 sources: 18,800 news and business sources and 6,000 legal sources.

The NEXIS service is the largest news and business online information service, with not only news, but company, country, financial, and demographic information, as well as market research and industry reports. The NEXIS service is unmatched in depth and breadth of information. In fact, 120,000 new articles are added each day from worldwide newspapers, magazines, news wires and trade journals.

Although the overwhelming majority of the information sources on the LEXIS and NEXIS services are public in nature, all of which are available to the general public through their public libraries, the local news stand or bookstore, or from government offices, a handful of the data sources that contribute to our services are not available to the general public. These data sources include consumer credit reporting files but contain only basic identifying information (*e.g.*, name, address) that is used by customers of LEXIS and NEXIS to locate specific individuals.

LEXIS-NEXIS also is a founding member of the Individual Reference Services Group (IRSG), which represents leading information industry companies, including the three major credit reporting agencies, that provide commercial information services to help verify the identity of or locate individuals. Each of the member companies has adopted self-regulatory principles governing the dissemination and use of personal data, principles which the IRSG developed in 1997 in conjunction with the Federal Trade Commission. While I will concentrate on LEXIS-NEXIS' practices, we believe that these are typical of the practices of members of the IRSG.

Our company and the other members of the IRSG are committed to the responsible acquisition and use of personally identifiable information, and share the Subcommittee's concern about the potential misuse of data for identity theft and other harmful purposes. Indeed, in the fight against identity theft, where verifying an individual's identity is crucial, individual reference service products are absolutely essential.

My remarks today will focus on three areas. First, because most people know relatively little about our industry and may confuse the sort of services that are the topic of this hearing with

the mainstream of the industry, I will explain the customer base and socially beneficial uses for individual reference information. For example, law enforcement agencies and fraud investigators are major users of these services, and at a 1997 FTC workshop on database privacy the Secret Service, the Treasury Department's Financial Crimes Enforcement Network ("FINCEN"), American Bankers Association, and National Retail Federation all testified to the importance of these services for their work preventing and pursuing fraud.

Second, I will provide some background about the IRSG principles and their enforcement mechanisms. I also will illustrate some of the IRSG principles by explaining how LEXIS-NEXIS implements them.

Finally, I will make some observations about the impact of sections 7 and 8 of S. 2328 upon LEXIS-NEXIS and other individual reference services.

II. Uses of Individual Reference Service Information

Individual reference services are companies that furnish timely and reliable information to identify and locate individuals. The information is used by governmental, private sector, and non-profit entities for a wide range of beneficial purposes.

Individual reference services, such as those provided by LEXIS-NEXIS, are often the only way that individuals with limited resources, through the assistance of a professional who has access to these services, can obtain critical information. LEXIS-NEXIS' customers are professionals, primarily in the fields of law, business, journalism, and law enforcement.

For example, law enforcement agencies use these services to locate criminals and witnesses to crimes, and to confirm identities. In fact, individual reference services play an important role in combating the very sorts of fraud that flow from personal financial information falling into the wrong hands. At the June 1997 FTC workshop examining reference services, witnesses from both FINCEN and the Financial Crimes Section of the U.S. Secret Service testified to the value and importance of these services for their work.

In the fight against identity theft, where verifying an individual's identity is crucial, individual reference service products are absolutely essential. Banks, credit card companies, and other types of credit institutions, as well as gas, electric, and telephone companies and governmental entities distributing public entitlement programs, are all becoming increasingly plagued by fraudsters who use an existing person's identity to illegally obtain products, services and money. The best, and perhaps only, means of preventing this type of fraud is to crosscheck through the use of personal identifying data, often provided by individual reference services. Since the victims of identity theft are not only the businesses that lose billions to various forms of identity theft per year, but also the consumers whose credit is often ruined by this insidious act, everyone directly benefits by this application of the personal identifying information provided by individual reference services.

Individual reference service products also are an important tool for other types of fraud prevention efforts by businesses. The insurance industry, for example, relies on individual reference service products to investigate fraudulent claims. Credit card companies and department stores use them to detect and limit credit card fraud. Banks use them to detect and report credit card fraud, insider abuse, and money laundering. Many businesses use them to minimize the risk of financial fraud when they receive an unusual order for delivery of merchandise. Other businesses use them when performing due diligence before engaging in a business venture with a little-known corporation in the increasingly mobile world economy. The Insurance Information

Institute reports that special investigation units save their companies about $10 for every dollar invested in them.

Reference services help people in many other ways. One of the most compelling is child support enforcement. Whereas government-compiled child support databases have encountered difficulties in some instances, individual reference services have proven to be invaluable in tracking down parents who are delinquent in these obligations. In this way, these services advance personal responsibility, give much-needed income to divorced parents and their children, help free families from welfare dependency, and provide an additional source of revenue to state welfare programs. Individual reference services can locate non-custodial parents quickly and inexpensively, even in circumstances where they move to a different state or begin using a different name. The Association for Children for Enforcement of Support ("ACES"), the leading child support advocacy organization, uses LEXIS-NEXIS' P-TRAK service to assist families–approximately 80 percent of whom are on welfare–in locating parents who have failed to meet legal child support obligations. ACES has reported tremendous success with the service, locating more than 75 percent of the "deadbeat" parents they sought, and helping families receive much-needed support.

Among the many other important uses of individual reference services are:

finding long-lost family members,

locating heirs to estates who have moved or changed their names through marriage,

locating pension fund beneficiaries who have left a company,

locating victims of fraud schemes or environmental hazards,

protecting consumers from unlicensed professionals and sham businesses,

locating blood, organ and bone marrow donors,

promoting the transparency of the political process by providing easy-to-search information on individuals' campaign donations,

locating witnesses, and

providing citizens with efficient, ready access to federal, state, and local government information.

From these examples, I hope the Subcommittee will appreciate the value of individual reference services.

III. The IRSG Approach

Privacy Protection

Rapid advances in technology, a highly mobile society, the need to prevent fraud, and other market demands for information have spurred increased reliance upon information services provided by companies like LEXIS-NEXIS. These changes in society and technology also have resulted in a heightened interest in the privacy considerations implicated by such services. At LEXIS-NEXIS we are attuned to these issues and have strongly committed to taking a leadership role in effectively addressing them.

Privacy protection in the United States has evolved in a way that offers individuals effective protections while, at the same time, not limiting the benefits of technological advances. The ability to preserve both of these important interests results from a network of different policies. These policies are tailored to provide protections in specific circumstances in order to prevent actual or potential abuses of personal information. This sectoral approach is preferable to an omnibus or "one-size-fits-all" privacy policy that would govern all industries. Addressing privacy issues within specific industry sectors has proven very effective in evolving and responding to changes in industry and society.

The IRSG Principles

The importance of defining privacy practices tailored to specific types of information is demonstrated in the IRSG principles.

In September 1996, in the closing hours of the 104th Congress, the Federal Trade Commission proposed a broad prohibition on the use of credit header information—non-financial identifying information obtained from a consumer reporting agency's database. Members of the individual reference service industry and those who rely on credit header information alerted Congress that such a prohibition would severely limit important uses of this information. As a result of arguments made by industry, regulatory efforts were postponed until a further study of the issues could be conducted.

This gave LEXIS-NEXIS the opportunity to join together with 13 other companies in the individual reference services industry to form the IRSG. The companies that comprise the IRSG are the leaders in providing information and assisting users in identifying and locating individuals. In close consultation with the Federal Trade Commission, the IRSG developed a comprehensive set of self-regulatory principles backed by third-party assessments and government enforcement that these companies follow.

These principles focus on non-public information, that is, information about an individual that is of a private nature and neither available to the general public nor obtained from a public record. For example, the principles govern information obtained from credit headers, such as social security numbers and addresses and telephone numbers.

Companies that sign on to the IRSG principles commit—among other things—to:

acquire individually identifiable information only from sources known as reputable,

restrict their distribution of non-public information through appropriate safeguards,

educate the public about their database services, and

furnish individuals with a copy of the information contained in services and products that specifically identifies them, unless the information is publicly available.

One of the safeguards on the distribution of non-public information is a prohibition on the display of social security numbers and dates of birth in individual reference service products distributed to the general public and, for products distributed to professional or commercial users, a prohibition on the display of such information unless truncated in an appropriate manner (*e.g.*, masking of the last four or more digits of social security numbers). This IRSG principle has helped reduce the availability of social security numbers for sale on the Internet.

Self-Regulation with "Teeth"

Third-party assessments backed by government enforcement provide real "teeth" for enforcing these principles. Enforcement rests on the following three pillars:

- Legal sanctions–Any company that holds itself out to the public as following the principles may be responsible under existing federal and state law if the company fails to live up to them. Both the Federal Trade Commission and state attorneys general can bring charges under Section 5 of the Federal Trade Commission Act and similar state laws against member companies that fail to adhere the principles.

- Cut-off of data supply–Signatories to these principles require by contract that all companies buying non-public data from

them for resale abide by the principles. Non-complying companies risk losing access to the data they need for their products or services. This is particularly significant in that it is estimated that IRSG signatories control 90% of all non-public information obtained from credit headers.

- Independent assurance reviews—Every IRSG company must undergo a third-party assessment to verify compliance with the principles. I will describe this in more detail below.

Information Practices

In the spirit of openness, the principles require individual reference services to have an information practices policy statement available to the public upon request. These statements describe:

- the types of information included,
- the types of sources from which that information is obtained,
- the nature of how the information is collected,
- the type of entities to whom the information may be disclosed, and
- the type of uses to which the information may be put.

This openness enables individuals to understand the reference service's use of the information it possesses. Individual reference services also inform individuals, upon request, of the choices available to limit access to or use of information about them contained in a company's products and services. Further, the principles require an individual reference service to provide information about the nature of public record and publicly available information that it makes available in its products and services and the sources of such information.

Third-Party Assessments

To help ensure that member companies do not make unsubstantiated assertions of compliance, the IRSG principles require that independent professional services conduct annual third-party assessments of their compliance. These independent professional services can be accounting firms, law firms, or security consultants who use the criteria developed by PriceWaterhouseCoopers for the IRSG.

When the principles were adopted in December 1997, these companies agreed that the assurance reviews would be completed within 15 months. I am pleased to report that this is the second consecutive year in which the companies that offer products that fall within the scope of the IRSG principles and subscribe to the principles have successfully undergone these assessments. As this milestone attests, the IRSG has made great strides through self-regulation to secure the benefits of information service resources and ensure effective protection of consumer privacy.

IV. LEXIS-NEXIS' Practices: The IRSG Principles at Work

In addition to the IRSG principles, LEXIS-NEXIS maintains its own code of fair information practices. While these practices are based upon LEXIS-NEXIS' policies, they also provide an example of how the IRSG principles are implemented.

A. LEXIS-NEXIS Acquires Information Only From Reputable Sources

Section II of the IRSG principles requires that information be acquired "from only sources known as reputable in the government and private sectors." IRSG members are specifically required "to understand an information source's data collection practices and policies before accepting information from that source."

The majority of the information contained in LEXIS-NEXIS databases is public record information. Moreover, a significant portion of the information we provide comes from publicly available information such as news reports. A few of our many databases contain some information from non-public sources, such as credit header information (the non-financial, individual identifying information derived from the top of a credit report).

At present, we do not provide individually identifiable financial information from non-public sources. However, as discussed above, the IRSG principles are sufficiently broad to encompass, and would apply to, any member company's provision of this sort of non-public information.

Because most of our services offer public records, in many cases LEXIS-NEXIS obtains information directly from the government entity that originated it. In addition to governmental sources, the information gathered for our databases is collected from a wide variety of other sources, some of which are large, well-known companies and smaller, lesser-known businesses. Regardless of the size of the source, in our acquisition of information, we must be confident that all of the information we obtain is owned by the sources and possessed in a legal manner. We review the data collection practices and policies of our sources before accepting information from them to determine whether the data they propose to furnish to us was compiled in a lawful and ethical manner. Furthermore, in order to continue to ensure the accuracy and acceptable origin of information in our databases, we also engage in occasional site visits to evaluate directly the information practices of the source.

In addition, Section III of the IRSG principles requires that "[r]easonable steps be taken to help assure the accuracy of information in individual reference services." LEXIS-NEXIS has embraced this as one of our core policies for many years and through the IRSG we have reaffirmed our commitment to this important principle. LEXIS-NEXIS strives to obtain or create exact reproductions of the machine-readable versions of public records as copied and maintained by the official custodian of the records. We enter into written contracts with all of our sources that contain provisions attesting to the accuracy of the information the source provides LEXIS-NEXIS. These provisions instill confidence that our information is accurate by providing both a deterrent

against providing us with inaccurate information, as well as recourse against sources that may violate these provisions.

LEXIS-NEXIS' commitment to accuracy, however, does not end with the contractual commitment from the source. We also engage in original source checks to verify that the source is in compliance with our agreement. From time to time LEXIS-NEXIS will go to the original jurisdiction where information is generated and compare samples of information obtained from the jurisdiction with the information provided to LEXIS by its source. This procedure allows us to measure the level of accuracy of our suppliers.

B. Security

Section VI of the IRSG principles requires signatories to maintain facilities and systems to protect information from unauthorized access and from persons who may exceed their authorization. LEXIS-NEXIS employs a wide array of measures to protect at all times the security of our products and the information obtained from our suppliers. Our security measures are deployed both within our computer systems and within our physical plant.

To establish security within our database system, we employ the most effective security programming available. We constantly evaluate our system looking for weaknesses in order to eliminate them and upgrade security.

Our physical plant also uses the most effective security available, including state of the art surveillance systems. Access to the various sections of our facilities is limited to authorized employees. This is done through the use of a "swipe-in"/"swipe-out" card system that allows us to account for individuals who are working in certain areas and the times that they are in these areas. Security guards, surveillance cameras, and other surveillance techniques also are employed. Our security system provides the highest level of accountability, and has proved extremely successful in eliminating unauthorized use of information. Additionally, all LEXIS-NEXIS employees are required to sign a non-disclosure agreement stating that they will not disclose confidential information to which they have access as part of their job responsibilities.

C. Selective and Limited Distribution

Section V of the IRSG principles addresses distribution of non-public information. Section V.A requires that individual reference services distribute non-public information only to qualified subscribers and sets out a lengthy set of conditions that determine these qualifications, as well as record-keeping requirements concerning subscribers.

All of our subscribers enter into formal agreements with LEXIS-NEXIS that define the limits and appropriate uses of information obtained from our databases. For example, in its customer agreements, LEXIS-NEXIS requires customers to agree contractually not to use information obtained from the databases for purposes that would violate the Fair Credit Reporting Act. In addition, a warning about FCRA restrictions is prominently visible to LEXIS-NEXIS customers before they access many of the databases contained in the public record library, as well as files containing non-public information. This warning states:

> The Fair Credit Reporting Act (15 U.S.C § 1681) prohibits use of information from this file to determine a consumer's eligibility for credit or insurance for personal, family or household purposes, employment or a government license or benefit.

To become a LEXIS-NEXIS subscriber, the prospective customer must furnish information including company/organization name, address, contact person and telephone number. We do not respond to anonymous requests for information, and we thus would be able to assist authorities in the event that subscribers were ever to misuse information.

V. Adverse Impact of Sections 7 and 8 of S. 2328

S. 2328 would directly affect individual reference services in two ways. First, section 7 would cut off the supply of the type of identifying information we obtain from consumer reporting agencies and use to help ensure accuracy in indexing and compiling disparate information. Second, section 8 would mandate that individual reference service companies enter a very different market than they ever sought to enter—the consumer market for public record information—as a condition of selling public record information to lawyers, law enforcement officials, journalists, and other professionals. These proposals are, at best, burdensome and unnecessary and, at worst, unconstitutional and harmful to consumers.

Section 7—Cutting Off the Supply of Identifying Information

In prohibiting consumer reporting agencies from supplying anything other than a consumer's name and current address without a "permissible purpose," as defined by the Fair Credit Reporting Act, section 7 would have the effect of cutting off identifying information that we use to index and organize disparate information. Distinguishing between "John Smiths" who live in the same town is far more effective when we have available to us prior addresses, age, and social security number information. These indexing and verification uses are critical to ensuring that the products we, and other IRSG members, offer to professional and government agencies contain accurate and complete information.

The use of social security number information for indexing and verification purposes is different than the display of such information in individual reference service products. As noted earlier, the IRSG principles prohibit the display of social security numbers and dates of birth in individual reference service products distributed to the general public and, for products distributed to professional or commercial users, prohibit the display of such information unless truncated in an appropriate manner.[1]

Cutting off the availability of social security numbers and similar identifying information for indexing and verification purposes is particularly ironic in light of the requirement in section 8, discussed below, that individual reference service companies provide consumers with copies of "their files," who in turn will probably review the information for accuracy and completeness.

---

[1] This IRSG principle has helped reduce the availability of social security numbers for sale on the Internet. The most common sources of such information today are Web sites operated by private investigators and Web sites selling "stale" information they obtained prior to the implementation of the IRSG principles.

Section 8—Consumer Review of Public Record Information in their "Files"

Requiring individual reference service providers, upon request, to disclose to a consumer "the nature, content, and substance of all information in the file maintained by the provider," is unnecessary, burdensome, and unwise.

Section 8's requirement is unnecessary insofar as the IRSG's access principle already requires an individual reference service to provide an individual with "non-public information contained in" its look-up products that specifically identifies him or her. (Two types of information are exempted from this requirement: information obtained on a limited use basis from a governmental agency and information whose disclosure is limited by law or legally recognized privilege.)

For public record information (and publicly available information) contained in an individual reference service's products, the IRSG principles require a company, upon request, to advise an individual about the nature of such information that it makes available in its products and the sources of such information. Public record information is information about or related to an individual that has been obtained originally from the records of a federal, state, or local government entity that are open for public inspection. Examples of public records include titles to real property, real property tax assessor records, bankruptcies, judgments, liens, state professional licenses, and death records.

When contacted by an individual concerning an alleged inaccuracy about that individual in its public record information, the IRSG principles further require an individual reference service company to inform the individual of the source of the information and, if reasonably available, where a request for correction may be directed. To be effective, any correction of errors must be made with the government entities that are the sources of this information. The task of individual reference services in this regard is to reflect reliably the data made available by the originating public record source.

Moreover, neither inaccuracies nor consumer harm are a significant issue in connection with individual reference services. Technological developments and quality assurance measures yield information that reliably mirrors the original public records. Furthermore, the FTC acknowledged in its 1997 Report to Congress on Individual Reference Services that "neither workshop participants nor commentators identified concrete evidence of harm linked directly to inaccurate records offered by look-up services." Nor has any evidence to the contrary emerged since 1997. In addition, statutory safeguards do exist for individuals in the vast majority of circumstances in which the distribution of inaccurate public record information might cause them real harm. For example, the Fair Credit Reporting Act already regulates extensively the use of public record information in connection with decisions about a consumer's eligibility for employment, credit, or insurance.

Weighed against this dearth of evidence of inaccuracies or consumer harm is the enormous potential burden associated with retrieving potentially relevant information from the large number of databases of public records and verifying that it pertains to the individual making the request. This is necessary because many individual reference services, unlike consumer reporting agencies, do not maintain "files" in connection with specific individuals. For example, individual reference services leave to their customers the tasks of formulating their search inquiries, of personally reviewing the search results to determine whether the search might have been under-inclusive and, where the search inquiry is over-inclusive, of personally reviewing the search results to determine what records may be relevant. To meet the bill's demands, however, individual reference services

would need to hire teams of customer service representatives, train them, and assume the risk of error in formulating search inquiries and making associated decisions. In short, it would force individual reference services to assume risks they long ago shifted to their customers.

Finally, section 8 would require that, as a condition of selling public record information to lawyers, law enforcement officials, journalists, and other professionals, individual reference services enter the consumer market for public record information. This is a very different market than most individual reference services ever sought to enter. Moreover, imposing this condition would run afoul of the First Amendment because it would unduly burden the publication of information already in the public domain. *See, e.g.,* The Florida Star v. B.J.F., 491 U.S. 524 (1989) (striking down statute that imposed civil liability upon a newspaper for publishing the name of a rape victim which it had obtained from a publicly released police report); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979) (finding unconstitutional the indictment of two newspapers for violating a state statute forbidding newspapers to publish the name of any youth charged as a juvenile offender).

VI. Conclusion

Our company and the IRSG are committed to the responsible acquisition and use of personally identifiable information, and share the Subcommittee's concern about the potential misuse of data for identity theft and other harmful purposes. Nevertheless, individual reference service products are absolutely essential in the fight against identity theft, and the Congress should not take any steps that would jeopardize the usefulness of such services.